ABSTRACT

There is provided a method for recovering the complete coordinate of the scalar-multiplied point from partial information of the scalar-multiplied point given in a fast scalar multiplication method. Thereby, during calculation of the scalar-multiplied point in an elliptic curve defined on a finite field with characteristic of 5 or more, first the fast scalar multiplication method is used to give the partial information of the scalar-multiplied point, and the complete coordinate of the scalar-multiplied point is recovered from the result and outputted, so that the complete coordinate can be given at a high speed.